Todd M. Friedman (SBN 216752)
Adrian R. Bacon (SBN 2803320)
LAW OFFICES OF TODD M. FRIEDMAN, P.C.
21031 Ventura Blvd., Suite 340
Woodland Hills, CA 91364
Phone: 323-306-4234
Fax: 866-633-0228
tfriedman@toddflaw.com
abacon@toddflaw.com

PACIFIC TRIAL ATTORNEYS
A Professional Corporation
Scott J. Ferrell, Bar No. 202091
sferrell@pacifictrialattorneys.com
4100 Newport Place Drive, Ste. 800
Newport Beach, CA 92660
Tel: (949) 706-6464
Fax: (949) 706-6469

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

SONYA VALENZUELA, individually and on behalf of all others similarly situated,

Plaintiff,

v.

MICRON TECHNOLOGY, INC., a Delaware corporation d/b/a WWW.CRUCIAL.COM,

Defendant.

Case No. 2:23-cv-07058-FMO-PVC

FIRST AMENDED CLASS ACTION COMPLAINT

INTRODUCTION

Defendant has secretly installed a collection of surveillance tools on its website at www.crucial.com to identify every anonymous visitor. Defendant enables the companies that host these tools to intercept and extract a user's personal data so that Defendant can identify users and their online behavior. Defendant (and the companies that host these tools) then exploit their knowledge of visitors' identities, habits, and chat topics to bombard visitors with targeted marketing, including unwanted telephone calls and e-mails.

Moreover, Defendant allows third parties to wiretap and intercept communications directed from a user to Defendant's automated customer service chat bot. These communications are stored, analyzed, and interpreted by these third parties. Defendant does all of this without visitors' effective informed consent. As a result, Defendant has violated numerous laws.

JURISDICTION AND VENUE

1. Jurisdiction is proper pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1132(d), because the proposed class contains at least one hundred members, and the amount in controversy exceeds $5,000,000.

2. Venue is proper in this District because this matter was initially filed in the Superior Court of the State of California for the County of Los Angeles, and was since removed. The County of Los Angeles is within this judicial district.

PARTIES

3. Plaintiff is a resident of California. While physically within California within the past year, Plaintiff visited Defendant's Website using a smart phone and conducted a brief conversation with an agent of Defendant through the Website's chat feature. Plaintiff was not advised that the chat was monitored, intercepted, or recorded.

4. Defendant is a Delaware corporation with its principal place of business in Idaho. It sells computer memory and computer data storage products throughout the

United States via its website and other distribution channels. Defendant also owns and operates the above-referenced Website.

FACTUAL ALLEGATIONS

A. The Right to Privacy Has Always Been a Legally Protected Interest in the United States.

5. Since America's founding, privacy has been a legally protected interest at the local, state, and federal levels. *See Patel v. Facebook, Inc.*, 932 F.3d 1264, 1271–72 (9th Cir. 2019) (quoting *Spokeo, Inc. v. Robins*, 578 U.S. 330, 341 (2016)) ("Privacy rights have long been regarded 'as providing a basis for a lawsuit in English or American courts.'"); and *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 983 (9th Cir. 2017) ("Violations of the right to privacy have long been actionable at common law.").

6. More specifically, privacy protections against the disclosure of certain kinds of sensitive personal information are embedded in California statutes and at common law. *See e.g., U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 763 (1989) ("The Ninth Circuit has repeatedly held that privacy intrusions may constitute "concrete injury" for purposes of Article III standing); *Van Patten v. Vertical Fitness Grp., LLC*, 847 F.3d 1037, 1041–43 (9th Cir. 2017) (finding "concrete injury" where plaintiffs claimed that unsolicited telemarketing calls "invade the privacy and disturb the solitude of their recipients*"); In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 599 (9th Cir. 2020) (finding "concrete injury" where Facebook allegedly tracked users' "personally identifiable browsing history" on third party websites); *Patel*, 932 F.3d at 1275 (finding "concrete injury" where plaintiffs claimed Facebook's facial-recognition technology violated users' privacy rights).

7. In short, privacy is—and has always been—a legally protected interest in many contexts, including specifically with regard to sensitive personal information. Thus, a defendant whose acts or practices violate consumer privacy inflicts an actionable "injury" upon an individual.

///

B. The Right to Privacy Includes The Right To Online Anonymity.

8. The right to privacy includes the right to anonymity online. *In Re Anonymous Online Speakers*, 661 F.3d 1168 (9th Cir. 2011). Indeed, the "free exchange of ideas on the Internet is driven in large part by the ability of Internet users to communicate anonymously." *Doe v. 2TheMart.com Inc.*, 140 F. Supp. 2d 1088, 1093 (W.D. Wash. 2001).

9. Consumer expectations regarding privacy reinforce the actionability of these rights. According to Pew Research Center nearly all Americans believe it is important to (1) be in control of who can get information about their online activities; (2) to not be tracked online without their consent; and (3) to be in control of what information is collected about them.

10. Accordingly, most people don't want their private online browsing to be associated with their public offline identities. This is because online anonymity gives the freedom to investigate, explore, and research without fear of social repercussions. In addition, online anonymity helps prevent security breaches, surveillance and intrusive web-tracking.

C. The De-Anonymization of Internet Users Poses a Serious Threat to Personal Privacy and the Internet.

11. In simple terms, de-anonymization is a process that involves cross-referencing anonymized data with "commercially available information" ("CAI") obtained from grey data markets to reveal an individual's identity. De-anonymization has been called the "the biggest privacy threat no one is talking about."[1]

12. As the Director of National Intelligence explained in a January 22, 2022 report (approved for public release on June 5, 2023) (the "DNI Report"), "the volume and sensitivity of CAI have expanded in recent years mainly due to the advancement of digital technology, including location-tracking and other features of smartphones and

[1] https://technoglitz.com/de-anonymization-is-the-biggest-threat-to-privacy-that-no-one-is-talking-about/ (last downloaded July 2023).

other electronic devices, and the advertising-based monetization models that underlie many commercial offerings available on the Internet."

13. The Director of National Intelligence concluded (1) that the existence of these practices poses a threat to national security since it is available to foreign governments since it "clearly provides intelligence value," and (2) that it "raises significant issues related to privacy and civil liberties."

14. The Director of National Intelligence concluded that the "single most important point" is that the expansion of CAI is "increasingly powerful for intelligence and increasingly sensitive for individual privacy and civil liberties" such that the Intelligence Community "needs to develop more refined policies to govern its acquisition and treatment."

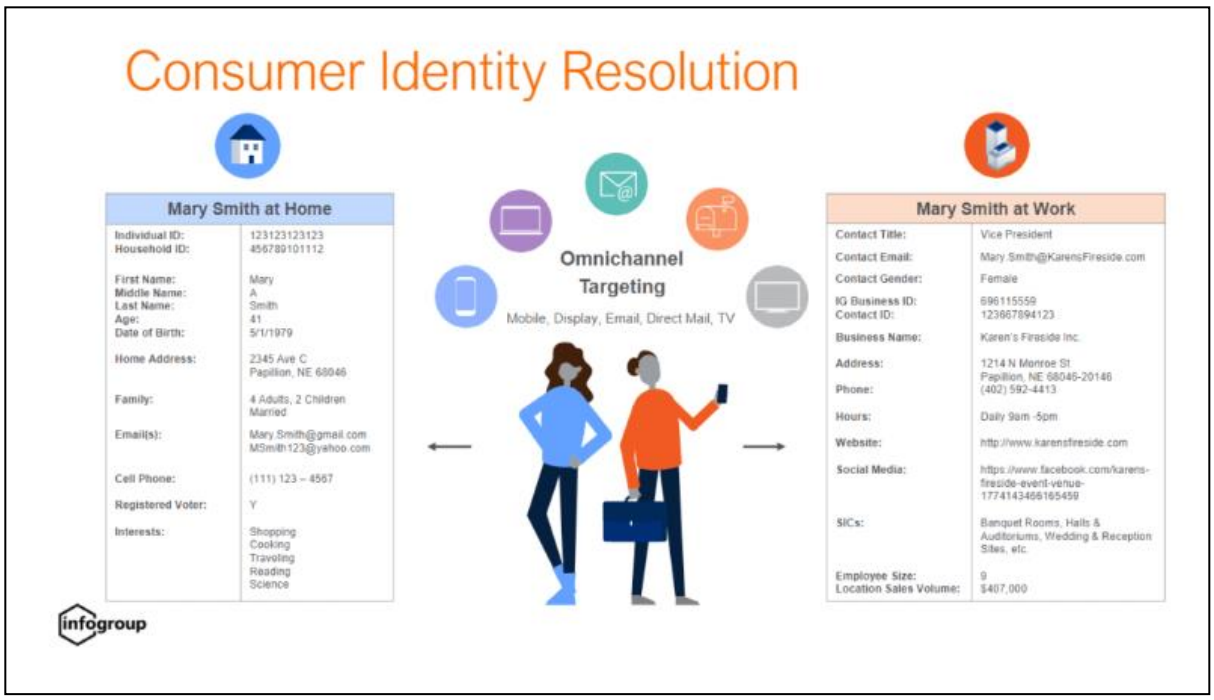
D. Defendant Uses "Identity Resolution" Malware Tools to Access Every Visitor's Device, Reveal Their Identities, and Publicize Their Personal Information to Its Marketing Partners.

15. As noted above, internet users have the right to remain anonymous. Nevertheless, some companies sell "identity resolution" tools to de-anonymize and track website visitors. Identity resolution is generally defined as "the ability to recognize an individual person, in real-time, by connecting various identifiers from their digital interactions across devices and touchpoints." *See* https://www.fullcontact.com/identity-resolution/ (last downloaded July 2023).

16. Identity resolution requires the collection of "technical markers" and other clues that digital visitors leave when they use the internet, even though most users "are trying to reveal as little information as possible." *See* https://venturebeat.com/ai/what-is-identity-resolution-its-benefits-challenges-and-best-practices/ (last downloaded July 2023). Those "technical markers" include routing information, locally stored data (sometimes called "cookies"), and idiosyncratic behavior of computers. The techniques have grown much more sophisticated over the years, and modern identity resolution algorithms rely upon dozens of types of details and digital footprints. *Id.*

17. In short, identity resolution providers aggregate visitor "touchpoints" containing anonymous identifiers to find links between the anonymous identifiers until the data compiled into a dossier about an anonymous individual can be linked to a specific individual by name, age, address, physical location, and more.

18. The following visual depiction shows an example of how identity resolution providers aggregate dozens of "touchpoints" to identify an anonymous internet user:



19. In the above example, the identity resolution provider has aggregated and analyzed dozens of anonymous "touchpoints" to reveal the following about a previously anonymous internet user, Mary Smith:

(a) Full name ***(Mary Smith)***

(b) Date of birth ***(May 1, 1979)***

(c) Gender ***(female)***

(d) Home address ***(2345 Avenue C, Papillion Nebraska)***

(e) Marital Status and Family ***(Married with two children)***

(f) E-mail address ***(Mary.Smith@gmail.com)***

(g) Personal Cell Phone: ***(111) 123-4567***

(h) Voter Registration Status ***(Registered)***

(i) Interests ***(Shopping, Cooking, Traveling, Reading, Science)***

(j) Employer ***(Karen's Fireside, Inc.)***

(k) Title ***(Vice President)***

(l) Work Hours ***(Daily 9-5)***

20. To identify each visitor, Defendant has several integrated identity resolution tools on its website, including:

a. Marketo,

b. Upsellit.com, and

c. Maxymiser

21. Each of these tools operates similarly: when a user accesses Defendant's website, each tool harvests certain data from the user's computer. For example, the Marketo tool harvests and records a user's IP address and device ID immediately upon a user accessing Defendant's website.

22. To illustrate: when a user connects to Defendant's website (or any website) certain data is automatically transmitted between a user's device and the website.

23. The transmission of this stream of data is required in order to create the network connection between the user and Defendant's website.

24. The Marketo tool is embedded in Defendant's website, and when a user connects to the website the tool intercepts and copies certain parts of this stream of data, such as the user's IP address and device ID. A network request is then sent from the Marketo tool—which is hosted on Defendant's website and servers—to Marketo's own servers which hosts a database of consumer information.

25. Marketo then compares the intercepted data with its own database (which consists of compiled data on consumers sourced from a myriad of places), to identify the user, determine their contact information, and deliver a comprehensive profile on that consumer to Defendant.

26. Marketo is also integrated with a platform called Liveramp, which is another identity resolution service.

27. Once Marketo has identified a consumer through the collection of their personal data, as described above, Defendant directs it to route this identification to Liveramp.

28. Liveramp then compares the consumer's information across multiple advertising networks to determine what kinds of targeted advertising that consumer is most likely to interact with.[2]

29. All of the above-mentioned tools operate similarly to Marketo and serve the same purpose: to identify a consumer based on intercepted data stored on their computer.

30. Each tool maintains its own database of consumer information, and so, on information and belief, Defendant utilizes each of them in order to generate the highest chance that a consumer can be identified from this intercepted data.[3]

31. The only reason any of this is possible is because Defendant has embedded the Marketo tool and other tools into its website and directed it to route this information to Liveramp.

32. Defendant profits from this by increasing its advertising revenue by showing users ads they are more likely to interact with.

33. Additionally, Defendant's website—through HTML code and without the use of a third-party tool—automatically accesses a user's locally stored data (such as cookies and device identifiers).

[2] Liveramp is able to do this by analyzing a user's online activity which is tracked across many websites. These websites collect a user's identifying information, similar to the way Defendant does, and then send that information to Liveramp. Liveramp compiles this information and creates a profile that describes what types of websites and information a particular consumer is interested in, which can then be used to determine what kinds of ads they might interact with.

[3] For example, if one database does not have information about and cannot identify a particular consumer, one of the others might be able to.

34. Defendant's website then creates a hidden connection between the user's web browser and a third-party website, such as MathTag.com, and allows this third-party website to collect the above-mentioned locally stored data.

35. All of this occurs before any consent has been requested by Defendant.

36. Within the statute of limitations period, Plaintiff visited Defendant's website and communicated with Defendant via Defendant's chat feature. As a result of Defendant's use of identity resolution malware and intrusion onto Plaintiff's device, Defendant: (1) obtained the IP address of Plaintiff; (2) identified Plaintiff's name, location, e-mail, browsing history, and other personal information; and (3) embedded Plaintiff's identity into the malware companies' database so that these companies can determine what ads Plaintiff was more likely to interact with.

37. As a result of Defendant's wrongful conduct: (1) Plaintiff has been de-anonymized and Plaintiff's personal information has been added to an extensive malware database; (2) Plaintiff has been bombarded with targeted advertising, e-mails, and telephone calls; (3) Plaintiff can no longer surf the web anonymously; and (4) Plaintiff has been exposed to heightened risk of identity theft.

38. In short, Defendant has deprived Plaintiff of numerous important privacy rights protected under California common law and statutes. Defendant's conduct amounts to "doxing by deanonymization" and robs Plaintiff of anonymity and obscurity. As a result, it is now easier for other companies to obtain other types of identity knowledge about Plaintiff and subject Plaintiff to further doxing. *See* *Doxing: A Conceptual Analysis, Ethics and Information Technology* (Volume 18, pages 199–210 (2016).

E. Defendant's Further Violation of California Invasion of Privacy Act.

39. In addition to de-anonymizing and doxing class members, Defendant also allows a third-party company to wiretap and eavesdrop upon class member communications through the website chat feature in violation of California law.

40. CIPA prohibits both wiretapping and eavesdropping of electronic communications without the consent of all parties to the communication. "'[T]he right to control the nature and extent of the firsthand dissemination of [one's] statements'" is viewed by the California Supreme Court "as critical to the purposes of Section 631[.]" *Javier v. Assurance IQ, LLC*, 2023 WL 114225, at *6 (N.D. Cal. Jan. 5, 2023) (Breyer, J.) (quoting *Ribas v. Clark*, 38 Cal. 3d 355, 361 (1985)); *Ribas*, 38 Cal. 3d at 360-61 ("a substantial distinction has been recognized between the secondhand repetition of the contents of a conversation and its simultaneous dissemination to an unannounced second auditor, whether that auditor be a person or mechanical device"). "[U]nder Section 631, it has always mattered who is holding the tape recorder[.]" *Javier*, 2023 WL 114225, at *6. Compliance with CIPA is easy, and most website operators comply by conspicuously warning visitors if their conversations are being recorded, intercepted, or eavesdropped upon.

41. Unlike most companies, Defendant *ignores* CIPA. Instead, Defendant enables and allows the third parties to eavesdrop on all such conversations. Why? Because, as one industry expert notes, "*Live chat transcripts are the gold mines of customer service. At your fingertips, you have valuable customer insight to make informed business decisions. . . .**When people are chatting, you have direct access to their exact pain points.***"). *See* https://www.ravience.co/post/improve-marketing-roi-live-chat-transcripts (last visited July 2023) (emphasis added).

42. To enable the eavesdropping, Defendant embedded a chat feature created using SalesForce's[4] Einstein Bots platform.

43. Einstein Bots is a service that allows companies—such as Defendant—to create AI-powered chat bots that they can then embed in their website to streamline customer service functions.

44. Bots created using SalesForce's Einstein Bots are powered by—i.e. hosted

[4] SalesForce is a third-party company specializing in cloud-based computing and customer relationship management.

on—SalesForce's Einstein 1 cloud computing platform.

45. As a result, any communications sent by a consumer to a chat bot created using Einstein Bots are automatically rerouted away from the original website and to SalesForce's Esintein 1 platform.

46. Then, SalesForce's Einstein 1 platform records the content of the messages for processing and analysis. This raw data is often stored for the use of both SalesForce and the companies that hire it to run their chat bot services.

47. SalesForce, after storing and compiling this data, analyzes the content of the chat messages in order to determine what automated response—if any—the chat bot should provide.

48. Once the chat bot determines the appropriate response to a user's input, that response is communicated back from SalesForce's Einstein 1 platform to the original website, where it appears in the chat system for the consumer to see.

49. Defendant hired SalesForce to host and/or operate its chat bot system, and to collect data on users of that chat bot system, as described above.

50. To that end, Defendant utilized the Einstein Bots platform to create a chat bot, hired SalesForce to host that chat bot on its Einstein 1 platform, and then embedded the chat bot in Defendant's own website so that consumers could interact with it.

51. Through this chat bot, Defendant redirects the inputs made by users to its chat bot system, in real time, from Defendant's own website to SalesForce's Einstein 1 platform.

52. SalesForce then records the inputs made by users of Defendant's chat bot system, analyzes them to determine what response the chat bot should give, and then communicates that response back to Defendant's website.

53. The only reason SalesForce is able to do any of this is because Defendant embedded the chat bot into its own website, and caused communications made to that chat bot to be routed to SalesForce's Einstein 1 platform. Had Defendant not done so, SalesForce would never receive any data whatsoever. Defendant, thus enabled

SalesForce to record, compile, and analyze the communications of website users.

54. Sales Force—at Defendant's direction—records every communication made to Defendant's chat bot by a user, and then analyzes those communications.

55. On information and belief, Defendant (and SalesForce) also utilize the Einstein 1 platform to analyze and aggregate consumer data which is, in part, collected through Defendant's chat system, as described above.

56. SalesForce does more than merely provide a storage function for Defendant regarding Website users' chat communications with Defendant. As shown above, SalesForce uses its record of Website users' interaction with Defendant's chat feature to enable targeted marketing by Defendant and the Identity Resolution Malware Companies.

57. Plaintiff accessed Defendant's website using her phone, and utilized Defendant's chat bot.

58. Plaintiff asked the chat bot several questions about Defendant's merchandise and services, particularly regarding hardware for her laptop.

59. Defendant, in real time, routed these messages from its chat bot to SalesForce's Einstein 1 platform.

60. SalesForce then recorded, processed, analyzed, and interpreted the messages in order to determine what response the chat bot should provide to Plaintiff.

61. Defendant did not inform Plaintiff or Class members that Defendant was secretly allowing, aiding, and abetting SalesForce to intercept and eavesdrop on the conversations during transmission.

62. Defendant did not obtain class members' effective consent for the preceding intrusions, nor were class members aware of Defendant's conduct.

CLASS ALLEGATIONS

63. Plaintiff brings this action individually and on behalf of all others similarly situated (the "Class") defined as follows:

All persons within the state of California who within the statute of limitations period: (1) visited Defendant's website; and (2) were exposed to the wrongful conduct described above.

64. NUMEROSITY: Plaintiff does not know the number of Class members but believes the number to be in the tens of thousands. The exact identities of Class members may be ascertained by the records maintained by Defendant.

65. COMMONALITY: Common questions of fact and law exist as to all Class members, and predominate over any questions affecting only individual members of the Class. Such common legal and factual questions, which do not vary between Class members, and which may be determined without reference to the individual circumstances of any Class member, include but are not limited to the following:

a. Whether Defendant engaged in the wrongful conduct described above;

b. Whether Plaintiff and Class members are entitled to statutory penalties; and

c. Whether Class members are entitled to injunctive relief.

66. TYPICALITY: As a person who visited Defendant's Website, whose privacy was invaded and whose electronic communication was recorded, intercepted and eavesdropped upon, Plaintiff is asserting claims that are typical of the Class.

67. ADEQUACY: Plaintiff will fairly and adequately protect the interests of the members of The Class. Plaintiff has retained attorneys experienced in the class action litigation. All individuals with interests that are actually or potentially adverse to or in conflict with the class or whose inclusion would otherwise be improper are excluded.

68. SUPERIORITY: A class action is superior to other available methods of adjudication because individual litigation of the claims of all Class members is impracticable and inefficient. Even if every Class member could afford individual litigation, the court system could not. It would be unduly burdensome to the courts in which individual litigation of numerous cases would proceed.

FIRST CAUSE OF ACTION

Violations of the California Invasion of Privacy Act

Cal. Penal Code § 631(a)

69. "Any person who, by means of any machine, instrument, or contrivance, or in any other manner, [i] intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system, or [ii] who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or [iii] who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or [iv] who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine . . . ." *Yoon v. Lululemon USA, Inc.*, 549 F. Supp. 3d 1073, 1080 (C.D. Cal. 2021) (Holcomb, J.) (line breaks and headings of clauses added for ease of reference) (quoting Cal. Penal Code § 631(a)).

70. Section 631 of the California Penal Code applies to internet communications and thus applies to Plaintiff's and the Class's electronic communications with Defendant's Website. "Though written in terms of wiretapping, Section 631(a) applies to Internet communications. It makes liable anyone who 'reads, or attempts to read, or to learn the contents' of a communication 'without the consent of all parties to the communication.'" *Javier v. Assurance IQ, LLC*, 2022 WL 1744107, at *1 (9th Cir. 2022); *Yoon*, 549 F. Supp. 3d at 1080 ("Courts agree … that CIPA § 631 applies to communications conducted over the internet.") (citing *Matera v. Google Inc.*, 2016 WL 8200619, at *18 (N.D. Cal. Aug. 12, 2016) (Koh, J.) (holding that second clause of section 631(a) "encompasses email communications, which pass over wires,

lines, or cables")); *In re Google Inc. Gmail Litig.*, 2013 WL 5423918, at *21 (N.D. Cal. Sept. 26, 2013) (Koh, J.) ("the Court finds that section 631 of CIPA applies to emails"); *In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d 797, 826 (N.D. Cal. 2020) (Labson Freeman, J.).

71. The software embedded on Defendant's Website to record and eavesdrop upon the Class's communications qualifies as a "machine, instrument, contrivance, or … other manner" used to engage in the prohibited conduct alleged herein. *See In re Facebook Internet Tracking Litig.*, 140 F. Supp. 3d 922, 937 (N.D. Cal. 2015) (stating that "***it is undeniable that a computer may qualify as a 'machine'***" within the meaning of section 631(a)) (emphasis added), *aff'd in part and rev'd in part on other grounds*, 956 F.3d 589 (9th Cir. 2020).

72. At all relevant times, Defendant intentionally caused the internet communication between Plaintiff and Class Members with Defendant's Website to be recorded. Defendant also aided and abetted, agreed with, employed, or conspired with SalesForce to wiretap and/or eavesdrop upon such conversations during transmission and in real time by voluntarily embedding the software code.

73. Defendant knows that SalesForce captures the electronic communications of visitors to Defendant's Website, and pays SalesForce to conduct these activities.

74. Plaintiff and Class Members did not expressly or impliedly consent to any of Defendant's actions.

75. A line of materially identical cases is pending in the Central District of California before the Honorable Sunshine S. Sykes. In the lead case, Judge Sykes held held that the above-described allegations state viable claims for violations of section 631(a) of CIPA. *See Byars v. The Goodyear Tire & Rubber Co.*, No. 5:22-cv-01358-SSS-KKx, 2023 WL 1788553, at *4 (C.D. Cal. Feb. 3, 2023) (Sykes, J.) ("*Byars contends that Goodyear, using a third-party service, "intercepts in real time" a website visitors' chat conversation. . . . Byars alleges that, using the chat conversation, website visitors share sensitive personal information. . . . . Because Byars has pled sufficient*

facts to show the contents of the communications and that the communications were intercepted, Byars has sufficiently stated a claim under § 631(a).") (emphasis added).

76. Defendant's conduct constitutes numerous discrete violations of Cal. Penal Code § 631(a), entitling Plaintiff and/or Class Members to injunctive relief and statutory damages.

SECOND CAUSE OF ACTION

CALIFORNIA UNAUTHORIZED ACCESS TO COMPUTER DATA ACT

PENAL CODE SECTION 502

77. The California Unauthorized Access to Computer Data Act (the "CUCA") makes it unlawful for parties to obtain data from a computer user outside of the scope of the user's authorization.

78. Specifically, Penal Code Section 502(c) imposes liability on any entity that "knowingly accesses and without permission" (1) uses any computer data, in order to "wrongfully control or obtain" computer data, or (2) "makes use of any data from a computer…"

79. CUCA provides a private right of action for compensatory damages, punitive damages, and attorneys' fees to any individual harmed by its violation. *See Facebook, Inc. v. Power Ventures, Inc.*, 2012 WL 542586 (N.D. Cal. Feb. 16, 2012).

80. By knowingly installing the Identity Resolution Malware to access class member devices and extract their personal information, Defendant violated CUCA. *See United States v. Christensen*, 828 F.3d 763, 789 (9th Cir. 2015) (violation of CUCA to access a device and use data improperly); and *Gilbert v. City of Sunnyvale* (2005) 130 Cal. App. 4th 1264, 1281 (accessing and without permission making use of any data from a computer system) violates CUCA.

THIRD CAUSE OF ACTION

CALIFORNIA INVASION OF PRIVACY

81. Article I, § 1 of the California Constitution provides, "All people are by nature free and independent and have inalienable rights. Among those are enjoying and

defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."

82. The phrase "and privacy" was added by an initiative adopted by California voters on November 7, 1972 (the Privacy Initiative). The Privacy Initiative created a private right of action against nongovernmental entities for invasions of privacy.

83. The California Supreme Court has explained that one of the principal "mischiefs" to which the Privacy Initiative was directed was "the overbroad collection and retention of unnecessary personal information by government and business interests." *White v. Davis*, 13 Cal.3d 757, 775 (Cal. 1975).

84. Defendant's conduct in secretly accessing class member devices, gathering highly personal details about them and their browsing history, and sharing that information with malware companies amounts to doxing and violates class members' rights to privacy.

85. Defendant assisted the malware companies to create etailed dossiers of class members and then share it with and sell it to numerous other companies.

86. Class members have the right to privacy in their web-browsing history; in how personal information is going to be used; in the right to withhold and not disclose personal information; and all statutory privacy rights codified under federal and California law.

87. Defendant has intruded on these privacy interests.

88. Defendant's actions constitute a serious invasion of privacy in that they violate several state laws; disclosed sensitive personal information to third parties; and facilitated the disclosure of class member information by third parties who did not have legal access to their personal information.

89. Defendant acted with oppression, fraud, or malice.

90. Class members have been damaged by Defendant's invasion of privacy and are entitled to just compensation in the form of actual and punitive damages.

FOURTH CAUSE OF ACTION

INTRUSION UPON SECLUSION

91. A claim for intrusion upon seclusion requires (1) intrusion into a private place, conversation, or matter; and (2) in a manner highly offensive to a reasonable person.

92. Defendant intentionally intruded upon class members' solitude and seclusion by (1) secretly accessing their devices to install identity resolution malware without their knowledge or permission; and (2) mining their personal data and sharing it with malware companies.

93. As set forth above, the right to online privacy is both actionable and expected by consumers. As such, Defendant's brazen de-anonymization of class members was highly offensive to all reasonable persons.

94. None of Defendant's actions were authorized.

95. Defendant violated state criminal and civil laws designed to protect individual privacy and against theft.

96. Defendant has acted with oppression, fraud, or malice.

97. Class members are entitled to just compensation in the form of actual damages and punitive damages under this cause of action.

FIFTH CAUSE OF ACTION

VIOLATION OF THE WIRETAP ACT, 18 U.S.C. § 2510, *et seq.*

98. Plaintiff incorporates by reference all of the above paragraphs as though fully stated herein.

99. The Wiretap Act, as amended by the Electronic Communications and Privacy Act of 1986, prohibits the intentional interception of any wire or electronic communication. Under 18 U.S.C. § 2520(a) there is a private right of action to any person whose wire, oral, or electronic communication is intercepted.

100. Plaintiff and Members of the Class were unaware that Defendant was intentionally causing their electronic communications to be intercepted. Defendant

intentionally caused technology to be utilized by other third-parties as a means of intercepting and acquiring the contents of Plaintiff's and Members of the Classes' electronic communications, in violate on of 18 U.S.C. § 2511.

101. As such, Plaintiff and members of the Class are entitled to preliminary, equitable, and declaratory relief, in addition to statutory damages of the greater of $10,000 or $100 per day for each violation, actual damages, punitive damages, and reasonable attorneys' fees and costs under 18 U.S.C. § 2520.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for the following relief against Defendant:

1. An order certifying the Class, naming Plaintiff as the representative of the Class and Plaintiff's attorneys as Class counsel;
2. An order declaring Defendant's conduct violates the above-referenced laws;
3. An order of judgment in favor of Plaintiff and the Class and against Defendant on the causes of action asserted herein;
4. An order enjoining Defendant's conduct as alleged herein and any other injunctive relief that the Court finds proper;
5. Statutory, actual, and punitive damages;
6. Reasonable attorneys' fees and costs; and
7. All other relief that would be just and proper as a matter of law or equity;

Plaintiff hereby demands a trial by jury on all issues so triable.

Dated: November 15, 2023 LAW OFFICES OF TODD M. FRIEDMAN, P.C.

By: s/Todd M. Friedman
Todd M. Friedman
Attorneys for Plaintiff

PROOF OF SERVICE

I, the undersigned, certify and declare that I am over the age of 18 years, employed in the county of Los Angeles, State of California, and not a party to the above-titled action. On November 15, 2023, I electronically filed with the Court through its CM/ECF system. Pursuant to the CM/ECF system, registration as a CM/ECF user constitutes consent to electronic service through the Court's transmission facilities. The Court's CM/ECF system sends an email notification of the filing to the parties and all counsel of record listed on the ECF page.

Executed on November 15, 2023, at Woodland Hills, CA.

I certify under the penalty of perjury that the foregoing is true and correct.

By: s/ Todd M. Friedman
Todd M. Friedman